UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,496	07/06/2001	Michael Freed	NEXSI-01110US0	4132

28863 7590 04/07/2006

SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,496	FREED ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are rejected.

Response to Arguments

2. Applicant's arguments filed on 10/17/05 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the prior art of record does not explicitly disclose application data being encrypted at application layer and decrypted at packet level of a network stack of the intermediate device without processing the application data with an application layer of a network stack. However, based on the interpretation of the examiner, the claim does not explicitly disclose that the application data is encrypted at application layer or packet layer, the claim simply discloses that receiving encrypted application data (which can be transmitted through application layer or packet layer) from the client. Therefore, applicant is advised to present argument that can be more clearly related to in the claims since the examiner examines the application with broadest interpretation.

Furthermore, the examiner's interpretation of the claim language has been described above. Therefore, dependent claims have been rejected based on the interpretation with respect to independent claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

4. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9, 12-15 and 18-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Friedman et al. US (6,240,513).

6. As to claim 1, 23 and 30: Jardin discloses A method for secure communications between a client and one of a plurality of servers performed on an intermediary device coupled to the client and said plurality of servers, comprising:

establishing an open communications session between the intermediary device and the client via an open network;(items 210, 220, 230 and 240 of FIG 2; describes the "handshake " between the client and the server which used to start any SSL communication between the server and the client)

negotiating a secure communications session with the client;(Col 6, lines 40-47)

establishing an open communications session with said one of said plurality of servers via a secure network;(Col 6, lines 40-47)

receiving encrypted application data from the client via the secure communications session; (Col 6, line 67;)

decrypting the encrypted application data; (Col 6, line 67)

forwarding the decrypted application data to the server via the secure network; (Col 7, line 4)

receiving application data from the server via the secure network;(Col 8. line 23-25)

encrypting the application data; and (Col 6, lines1-3 and items 250,260 of FIG.2)

sending encrypted application data to the client.(Col 8, lines 24-26)

detecting a communications anomaly in a communications session between the client and the intermediary device; and (Col 8, lines 31-35)

passing TCP data from through the intermediary device. (Col 4, lines 37-43) but Jardin doesn't explicitly disclose the steps (e) and (f) are performed at the packet level of a network stack of the intermediate device without processing the application data with an application layer of a network stack. However Friedman discloses a network security device responsible for establishing a secure session between two clients (Abstract) where he teaches the encryption/decryption and forwarding of packets are done on the packet level of the network stack of the device without reaching the application layer of the stack (*Col 5, lines 47-55 & Col 6, line 61 through Col 7, line 8*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Jardin system with the teachings of Friedman to perform the steps of encrypting/decrypting and forwarding the packets at the packet level of the network stack with processing application data with the application layer stack. One would be motivated to do so because such modification would enable the system to process the packet at any network-layer device like regular routers with nominal modification to the device. Furthermore this would improve the performance of the system because the device can encrypt/decrypt the packet without waiting for the application data packets to arrive and processed (*Col 7, lines 11-21*).

7. As to claim 2: Jardin discloses the method of claim 1 wherein said step (a) comprises the sub steps of:

receiving a request for a communications session from the client; (item 210 of FIG. 2) responding to the request for a communications session in place of the server; and (item 220 of FIG.2) establishing a secure communications session between the client and the intermediary device. (items 220,230 and 240 of FIG. 2 describes the "handshake " between the client and the server which used to start any SSL communication between the server and the client)

8. As to claim 3: Jardin discloses the method of claim 2 wherein said step of (a) comprises: receiving a TCP SYN packet from a client and responding to the SYN packet with appropriate responses as a proxy for the server. (Col 4, lines 39-41)

9. As to claim 4: Jardin discloses the method of claim 1 wherein said step of negotiating a secure communications session comprises negotiating an SSL session with the client in place of the server. (Col 6, lines 1-3)

10. As per claims 5, 7 and 22: The method of claim 1 further including:
Receiving the application data as a multi-segment records (*Col 6, lines 66-68*);
Forwarding at least a portion of the decrypted application for each of the records prior to receiving complete records(*Col 7, lines 3-5*); but he doesn't disclose discarding at least a portion of each of the record after forwarding; and Authenticating the decrypted application data of each data record using the remaining non-discarded portion of the data record upon receiving a final segment of the multi-segment record. However Friedman discloses a However Friedman discloses a network security device responsible for establishing a secure session between two

clients (Abstract) where he teaches discarding a portion of the record after forwarding (Col 12, lines 43-49 & Col 13, lines 12-21) and authenticating the decrypted application data using the remaining portion of the data (Col 16, lines 14-36). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Jardin system with the teachings of Friedman to discard a portion of the record after forwarding and authenticating the decrypted application data. One would be motivated to do so because discarding portion of the record and authenticating the remaining portion will enable the system to identify and discard records that have been altered or modified without processing the complete record.

11. As to claim 6 : Jardin discloses the method of claim 1 wherein the step of forwarding decrypted application data to said one of said plurality of servers comprises forwarding unauthenticated application data. (Col 7, line 4)

12. As to claims 8 and 14 : Jardin teaches the method of claim 1 wherein, prior to said step establishing a communications session with one of said plurality of servers, the method includes the step of:

selecting one of said plurality of servers to forward said decrypted authentication data to based on a load-balancing algorithm that calculates current processing loads associated with each of the servers. (*Col 8, lines 27-67 through Col 9 line 10; Jardin teaches different algorithms in his embodiments to balance the load on the plurality of servers*)

13. As to claim 9: Jardin disclose the method of claim 8 further including the step of: tracking data passing between the client and said one of said plurality of servers. (Col 8, lines 31-33)

14. As to claim 12: Jardin disclose an apparatus coupled to a public network and a secure network, communicating with at least one client via the public network and communicating with one of a plurality of servers via the secure network, comprising:
a network interface communicating with the public network and the secure network;(Col 2, lines 57-65) at least one processor;(Col 6, lines 32-34) programmable dynamic memory addressable by the processor; a communications channel coupling the processor, memory and network communications interface; (Col 2, lines 57-65) a proxy TCP communications engine; (Col 4, lines 34-36) a proxy SSL communications engine; (Col 4, lines 24-29)) a server TCP communications engine; (Col 2, lines 54-65)and a packet data encryption and decryption engine. (Col 7, lines 29-32) but he doesn't disclose the proxy SSL communication engine and the server TCP communications engine decrypt encrypted application data from the client and forward the decrypted application data to the one of plurality of servers without processing the application data with an application layer of a network stack of the apparatus. However Friedman discloses a network security device responsible for establishing a secure session between two clients (Abstract) where he teaches the encryption/decryption and forwarding of packets are done on the packet level of the network stack of the device without reaching the application layer of the stack (*Col 5, lines 47-55 & Col 6, line 61 through Col 7, line 8*). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Jardin system with

the teachings of Friedman to perform the steps of encrypting/decrypting and forwarding the packets at the packet level of the network stack with processing application data with the application layer stack. One would be motivated to do so because such modification would enable the system to process the packet at any network-layer device like regular routers with nominal modification to the device. Furthermore this would improve the performance of the system because the device can encrypt/decrypt the packet without waiting for the application data packets to arrive and processed (*Col 7, lines 11-21*).

15. As to claim 13: Jardin disclose the apparatus of claim 12 further comprising a negotiation manager that enables the apparatus as a TCP and SSL proxy for the server. (Col 4, lines 24-29)

16. As to claim 15: Jardin disclose the apparatus of claim 12 wherein the encryption and decryption engine decrypts encrypted packet data to produce application data. (Col 6, line66 through Col 7 line 2)

17. As to claim 18: The apparatus of claim 16 further including a recovery manager using said database to recover from communication errors. (Col 8, lines 27-41)

18. As to claim 19: Jardin discloses the apparatus of claim 12 wherein the packet data encryption and decryption engine decrypts packets from SSL data which spans over multiple TCP segments and forwards packet data to a server which is not authenticated. (Col 7, Col 7, line 4 and lines 44-45; the examiner deeming the data spanning over multiple TCP segments to

be inherent to any TCP/IP system, which split the application data packets to multiple TCP/IP packets to be transmitted over the network.)

19. As to claim 20: Jardin disclose the apparatus of claim 12 wherein said data is not buffered during decryption. (Col 3, lines 4-13 / in one embodiment the first server is configured to decrypt contents of the data packet and re-direct the data packet)

20. As to claim 21: The apparatus of claim 12 wherein said data is buffered for a length sufficient to complete a block cipher used to encrypt the data.(Col 2, lines 65, through Col 3, line 3 / the broker in the second embodiment have dynamically allocated buffer)

21. As to claim 24: Jardin system discloses the method of claim 23 wherein the secure communication is SSL protocol encrypted application data. (Col 4, lines 54-56)

22. As to claim 25: Jardin system discloses the method of claim 23 wherein said step of receiving comprises the sub steps of initiating a communications session with the enterprise and negotiating a secure communication session with the device.(items 210, 220, 230 and 240 of FIG 2; describes the "handshake " between the client and the server which used to start any SSL communication between the server and the client)

23. As to claim 26: Jardin system discloses the method of claim 23 further including the step of negotiating an open communication session with said at least one server of the enterprise and

wherein said step of forwarding includes forwarding decrypted data via the open communication network. (Col 6, lines 40-47 and Col 7, line 4)

24. As to claim 27: Jardin discloses the method of claim 23 wherein said step of receiving communications includes receiving a plurality of secure communication sessions from a plurality of customers. (Col 4, lines 11-16)

25. As to claim 28: Jardin discloses the method of claim 27 further including a step of selecting one of a plurality of enterprise servers to which to direct data in said step of forwarding said decrypted packet data.(Col 8, lines 27-67 through Col 9 line 10)

26. Claims 10,11,16,17 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Friedman et al. US (6,240,513) as applied to claim 1 above, and further in view of Abramson et al US (6,539,494).

27. As per claims 10, 11, 16, 17 and 29: the as modified in claim 1 does not explicitly explain establishing a database to track session information to track TCP and SSL communication. However Abramson et al teaches the using and tracking of session information database tracking TCP SSL and other packet information (column 1, line 62, through column 2, line 18) and use it to recover from communication errors. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Abramson to backup and track session information in communication between client

and a server. One would be motivated to do so in order to enable the system to recover from communication failures transparently (Col 4,lines 55-67) and reconstitute the session data into a new session without loss of data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

GUY LAMARRE
PRIMARY EXAMINER